UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/940,985	08/29/2001	Masahiro Kaminaga	NIT-294	5972

7590 10/19/2006

MATTINGLY, STANGER & MALUR, P.C.
Suite 370
1800 Diagonal Road
Alexandria, VA 22314

EXAMINER	
DAVIS, ZACHARY A	
ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 10/19/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/940,985	**Applicant(s)** KAMINAGA ET AL.
	Examiner Zachary A. Davis	**Art Unit** 2137

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _01 August 2006_.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _1-13_ is/are pending in the application.

4a) Of the above claim(s) _1-4_ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _5-13_ is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _20060801_.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

1. A response was received on 01 August 2006. By this response, Claims 5, 6, and 11 have been amended. No claims have been added or canceled. Claims 1-4 were previously withdrawn from further consideration as being drawn to a nonelected invention. Claims 5-13 are currently under consideration in the present application.

Response to Arguments

2. Applicant's arguments filed 01 August 2006 have been fully considered but they are not persuasive.

Regarding the rejection of Claims 5-10 under 35 U.S.C. 112, first and second paragraphs, Applicant argues that the amendments to Claims 5 and 6 overcome the noted rejections. The Examiner notes that the amendments appear to overcome the issues of indefiniteness under 35 U.S.C. 112, second paragraph, and therefore such rejection is withdrawn. However, the Examiner further notes that Claims 5 and 6 still recite the limitation "in order of bit sequence" of data A or B. The Examiner again notes that the phrase "bit sequence" does not appear in the specification. Although Applicant points to Figure 22 and its related description for support of the limitation (see pages 9-10 of the present response), the cited portions do not mention the term "bit sequence" at all, nor do they explicitly appear to describe the order in which the bits are processed.

The Examiner notes that the amendments to Claims 11-13 raise new issues of indefiniteness and failure to comply with the written description requirement, and thus those claims are rejected as set forth below.

Regarding the rejection of Claims 11-13 under 35 U.S.C. 102(e) as anticipated by Kocher et al, US Patent 6327661, Applicant argues that Kocher only teaches "random selection of an input data bit and relocation thereof" and not the claimed invention (page 11 of the present response). Applicant further argues that "both data A and data B are significant data"; however, the Examiner notes that nowhere is this claimed, nor is it disclosed in the specification (the word "significant" does not appear in the specification at all). It appears that "significant data" is intended to contrast with the blinding data at the portion of Kocher cited by Applicant (column 12, lines 45-60), but again the Examiner notes that it is neither claimed nor disclosed in the specification that any data is "significant". Thus, this distinction is moot.

Applicant also argues that "data A has an associated relationship with data B, whereas Kocher's input data has no such association with the blinding data" (page 11 of the present response). However, the Examiner notes that the phrase "associated relationship" also appears nowhere in the claims or specification. The Examiner assumes that this "associated relationship" is intended to refer to the limitation in the claim that there is an operation unit in data B that corresponds to an operation unit in data A. However, the Examiner notes that there is a correspondence between operation units in the two sets of data in Kocher, as well; each input data bit has a corresponding blinding bit (column 12, lines 46-60, as previously cited), and this appears to correspond to the "associated relationship" as argued by Applicant. The Examiner further notes that as the permutation data is initialized, the sets of data are associated with each other (see column 12, lines 26-44).

Applicant additionally argues that the blinding data in Kocher is "temporarily generated" (page 11 of the present response). The Examiner fails to appreciate this argument, as that phrase does not appear in Kocher, and Applicant does not further elaborate the point.

Finally, Applicant argues that "[n]either data A nor data B are randomly arranged bits ... unlike Kocher's blinding data, and thus both data A and data B are significant". In response, the Examiner first notes that significant data can, in fact, be random; for example, cryptographic keys are often random numbers, but keys would definitely be considered significant data. Further, the Examiner notes that it appears likely that at least one of data A or data B would be a cryptographic key, given that a stated object of the present invention (i.e. tamper-resistant method) is to prevent the discovery of a key (see page 5, line 22-page 6, line 19 of the present specification). The Examiner also notes that it is well known that the strongest cryptographic keys are random values. Therefore, it appears likely that at least one of data A or data B would be a random value, and thus the limitation that data A and data B are not randomly arranged appears to contradict the specification.

Therefore, for the reasons detailed above, the Examiner maintains the rejections as set forth below.

Information Disclosure Statement

3. The information disclosure statement filed 01 August 2006 fails to comply with the provisions of 37 CFR 1.97, 1.98 and MPEP § 609 because each publication is not identified by publisher, author (if any), title, relevant pages, date, and place of publication, as required by 37 CFR 1.98(b)(5). It has been placed in the application file, but the information referred to therein has not been considered as to the merits. Applicant is advised that the date of any re-submission of any item of information contained in this information disclosure statement or the submission of any missing element(s) will be the date of submission for purposes of determining compliance with the requirements based on the time of filing the statement, including all certification requirements for statements under 37 CFR 1.97(e). See MPEP § 609.05(a).

Specification

4. The objection to the specification is maintained as set forth below for the reasons detailed above in reference to the rejections under 35 U.S.C. 112, first paragraph.

5. The specification is objected to as failing to provide proper antecedent basis for the claimed subject matter. See 37 CFR 1.75(d)(1) and MPEP § 608.01(o). Correction of the following is required: Claims 5 and 6 recite the limitation of transferring data "in order of bit sequence" of data A or B. There is no written description for such a limitation in the specification. Further, Claim 11 recites the limitation "wherein neither

said data A nor said data B are randomly arranged bits"; there is no written description for such a limitation in the specification. See below regarding the rejections under 35 U.S.C. 112, first paragraph, for further detail.

Claim Rejections - 35 USC § 112

6. As noted above, the rejection of Claims 5-10 under 35 U.S.C. 112, second paragraph, as indefinite, is withdrawn in light of the amendments to the claims. The rejection of Claims 5-10 under 35 U.S.C. 112, first paragraph, is maintained as set forth below for the reasons detailed above. The amendments to Claims 11-13 also raise issues of indefiniteness and failure to comply with the written description requirement, and therefore those claims are also rejected as set forth below.

7. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

8. Claims 5-13 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

Claims 5 and 6 include limitations not described in the specification. Specifically, Claim 5 recites transferring an operation unit in the bit pattern of data A or B “in order of bit sequence” of data A or B, and Claim 6 recites transferring an operation unit of data A or B “in order of bit sequence” of data A or B. There is no explicit description of data transfer in order of a bit sequence. Further, it appears that the term “bit sequence” does not appear anywhere in the specification.

Claim 11 has been amended to include limitations not described in the specification; specifically, Claim 11 now recites “wherein neither said data A nor said data B are randomly arranged bits”. There is no description that data A or B cannot be randomly arranged bits in the specification. Further, the phrase “randomly arranged” appears nowhere in the specification. Further, as noted below regarding the rejection under 35 U.S.C. 112, second paragraph, the negative limitation renders the claim indefinite, and the limitation appears to contradict the specification.

Claims not specifically referred to above are rejected due to their dependence on a rejected base claim.

9. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

10. Claims 11-13 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 11 has been amended to recite the limitation "wherein neither said data A nor said data B are randomly arranged bits". The Examiner notes that this negative limitation, i.e. claiming what the data is NOT, renders the claim indefinite, because it is not clear from the claims or specification exactly in what ways data A or B are arranged, if not randomly. Further, the Examiner notes that the specification describes in several places the use of keys for encryption. It appears that data A or B would likely be a key if one were using the claimed tamper-resistant method, given that a stated object of the present invention is to prevent the discovery of a key (see page 5, line 22-page 6, line 19 of the present specification); the Examiner further notes that it is well known that the strongest key is, in fact, a random number (i.e. arrangement of bits). Therefore, the limitation that neither data A nor B is randomly arranged bits appears to contradict the specification; this contradiction further renders the claim indefinite.

Claims 12 and 13 are rejected due to their dependence on a rejected base claim.

Claim Rejections - 35 USC § 102

11. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

12. Claims 11-13 are rejected under 35 U.S.C. 102(e) as being anticipated by Kocher et al, US Patent 6327661.

In reference to Claims 11 and 12, Kocher discloses a tamper-resistant processing method including randomly selecting an unprocessed operation unit in data A corresponding to a generated random number, executing an arithmetic operation on the unit of the data A and a corresponding unit of data B, storing the result, and repeating the above steps until the operation has been completed (column 10, line 50-column 13, line 20; noting particularly column 10, lines 57-59, column 12, lines 13-19, and column 13, lines 11-20).

In reference to Claim 13, Kocher further discloses that the arithmetic operation can be one of logical AND, OR, or XOR (see column 12, lines 45-60).

Allowable Subject Matter

13. Claims 5-10 would be allowable if rewritten or amended to overcome the rejection(s) under 35 U.S.C. 112, first paragraph, as set forth in this Office action.

14. Reasons for indicating allowable subject matter were set forth in the previous Office action.

Conclusion

15. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Zachary A. Davis whose telephone number is (571) 272-3870. The examiner can normally be reached on weekdays 8:30-6:00, alternate Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

ZAD
zad

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER